FORM PTO-1390 (Modified)
(REV 11-2000)

U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371

ATTORNEY'S DOCKET NUMBER
PF990030

U.S. APPLICATION NO. (IF KNOWN, SEE 37 CFR
09/926585

INTERNATIONAL APPLICATION NO.	INTERNATIONAL FILING DATE	PRIORITY DATE CLAIMED
PCT/EP00/04053	**05 May 2000 (05.05.00)**	**01 June 1999(01.06.99)**

TITLE OF INVENTION
DIGITAL DATA WATERMARKING SYSTEM USING NOVEL WATERMARK INSERTION AND DETECTION METHODS

APPLICANT(S) FOR DO/EO/US
Teddy Furon and Pierre Duhamel

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☒ This is an express request to begin national examination procedures (35 U.S.C. 371(f)). The submission must include itens (5), (6), (9) and (24) indicated below.
4. ☐ The US has been elected by the expiration of 19 months from the priority date (Article 31).
5. ☒ A copy of the International Application as filed (35 U.S.C. 371 (c) (2))
   a. ☐ is attached hereto (required only if not communicated by the International Bureau).
   b. ☒ has been communicated by the International Bureau.
   c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US).
6. ☐ An English language translation of the International Application as filed (35 U.S.C. 371(c)(2)).
   a. ☐ is attached hereto.
   b. ☐ has been previously submitted under 35 U.S.C. 154(d)(4).
7. ☒ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371 (c)(3))
   a. ☐ are attached hereto (required only if not communicated by the International Bureau).
   b. ☐ have been communicated by the International Bureau.
   c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
   d. ☒ have not been made and will not be made.
8. ☐ An English language translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
9. ☒ An oath or declaration of the inventor(s) (35 U.S.C. 371 (c)(4)).
10. ☐ An English language translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371 (c)(5)).
11. ☒ A copy of the International Preliminary Examination Report (PCT/IPEA/409).
12. ☒ A copy of the International Search Report (PCT/ISA/210).

Items 13 to 20 below concern document(s) or information included:

13. ☒ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
14. ☐ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
15. ☒ A **FIRST** preliminary amendment.
16. ☐ A **SECOND** or **SUBSEQUENT** preliminary amendment.
17. ☐ A substitute specification.
18. ☐ A change of power of attorney and/or address letter.
19. ☐ A computer-readable form of the sequence listing in accordance with PCT Rule 13ter.2 and 35 U.S.C. 1.821 - 1.825.
20. ☐ A second copy of the published international application under 35 U.S.C. 154(d)(4).
21. ☐ A second copy of the English language translation of the international application under 35 U.S.C. 154(d)(4).
22. ☒ Certificate of Mailing by Express Mail
23. ☒ Other items or information:

    Return Postcard Receipt

U.S. APPLICATION NO. (IF KNOWN, SEE 37 CFR	INTERNATIONAL APPLICATION NO.	ATTORNEY'S DOCKET NUMBER
09/926585	PCT/EP00/04053	PF990030

24. The following fees are submitted:.

BASIC NATIONAL FEE (37 CFR 1.492 (a) (1) - (5)) :

		CALCULATIONS	PTO USE ONLY
□ Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO and International Search Report not prepared by the EPO or JPO	**$1040.00**		
☒ International preliminary examination fee (37 CFR 1.482) not paid to USPTO but International Search Report prepared by the EPO or JPO	**$890.00**		
□ International preliminary examination fee (37 CFR 1.482) not paid to USPTO but international search fee (37 CFR 1.445(a)(2)) paid to USPTO	**$740.00**		
□ International preliminary examination fee (37 CFR 1.482) paid to USPTO but all claims did not satisfy provisions of PCT Article 33(1)-(4)	**$710.00**		
□ International preliminary examination fee (37 CFR 1.482) paid to USPTO and all claims satisfied provisions of PCT Article 33(1)-(4)	**$100.00**		
ENTER APPROPRIATE BASIC FEE AMOUNT =		**$890.00**	
Surcharge of **$130.00** for furnishing the oath or declaration later than □ 20 □ 30 months from the earliest claimed priority date (37 CFR 1.492 (e)).		**$0.00**	

CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE		
Total claims	11 - 20 =	0	x $18.00	**$0.00**	
Independent claims	4 - 3 =	1	x $84.00	**$84.00**	
Multiple Dependent Claims **(check if applicable).**			□	**$0.00**	
TOTAL OF ABOVE CALCULATIONS =				**$974.00**	
□ Applicant claims small entity status. See 37 CFR 1.27). The fees indicated above are reduced by 1/2.				**$0.00**	
SUBTOTAL =				**$974.00**	
Processing fee of **$130.00** for furnishing the English translation later than □ 20 □ 30 months from the earliest claimed priority date (37 CFR 1.492 (f)). +				**$0.00**	
TOTAL NATIONAL FEE =				**$974.00**	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31) **(check if applicable).** □				**$0.00**	
TOTAL FEES ENCLOSED =				**$974.00**	
				Amount to be: refunded	$
				charged	$

a. □ A check in the amount of ______________ to cover the above fees is enclosed.

b. ☒ Please charge my Deposit Account No. **07-0832** in the amount of **$974.00** to cover the above fees. A duplicate copy of this sheet is enclosed.

c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. **07-0832** A duplicate copy of this sheet is enclosed.

d. □ Fees are to be charged to a credit card. **WARNING:** Information on this form may become public. **Credit card information should not be included on this form.** Provide credit card information and authorization on PTO-2038.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

Mr. Joseph S. Tripoli
THOMSON multimedia Licensing Inc.
Patent Department
PO Box 5312
Princeton, New Jersey 08540

SIGNATURE

DAVID T. SHONEMAN
NAME

39,371
REGISTRATION NUMBER

November 21, 2001
DATE

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant	:	Teddy Furon and Pierre Duhamel
Filed	:	Herewith
For	:	DIGITAL DATA WATERMARKING SYSTEM USING NOVEL WATERMARK INSERTION AND DETECTION METHODS

PRELIMINARY AMENDMENT

Hon. Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231

Sir:

In the US national phase application of PCT/EP00/04053 filed herewith, please enter the following amendments:

IN THE SPECIFICATION:

Please amend the specification as follows:

On Page 1, line 3, please insert the following paragraph:

-- This application claims the benefit, under 35 U.S.C. § 365 of International Application PCT/EP00/04053, filed May 5, 2000, which was published in accordance with PCT Article 21(2) on December 7, 2000 in English and which claims the benefit of French patent application No. 9907139 filed June 1, 1999.--

IN THE CLAIMS:

Please amend the claims as follows. A marked-up version of the claims is attached herewith.

1. Method for inserting a watermark into data (**x**) representing a content to be protected, comprising the steps of:

a) supplying a pseudo random noise sequence (**v**) to the input of a filter with predefined impulse response (**h**); and

b) adding said filtered pseudo noise sequence (**w**) to said data.

2. Method according to Claim 1, further comprising the steps of:

c) performing a pseudo random interleaving (p) of the data (**x**) before step b); and

d) performing an inverse interleaving after step b) so as to obtain the watermarked data.

3. Method for detecting a watermark in data (**r**) representing a content received, comprising the steps of:

i) performing a spectral analysis of said data; and

ii) deducing therefrom whether said data include a pseudo noise sequence which has been filtered by a filter with predefined spectral response (H(f)).

4. Method according to Claim 3 for detecting a watermark in data (**r**) representing a content received, the watermark being adapted to be inserted in accordance with the method according to Claim 2, furthercomprising:

iii) performing, before step i), a pseudo random interleaving (p) of the data (**r**) received, which is identical to the interleaving performed in step c).

5. Watermarking System using a watermark insertion method according to Claim 1 and a watermark detection method according to Claim 3, wherein a first series of parameters (**v**, **h**), the private key (K_{PRI}), is used for the insertion of the watermark and a second series of parameters (|H(f)|), the public key (K_{PUB}), is used for the detection of the watermark, so that:

knowledge of the public key does not make it possible to know the private key; and

knowledge of the watermark detection method and of the public key does not make it possible to delete or modify the watermark.

6. Device for inserting a watermark into data (**x**) representing a content to be protected, comprising:

means for generating a pseudo random noise sequence (**v**);

filtering means [(16)] having a predefined impulse response (**h**) and which are adapted for receiving said pseudo noise sequence (**v**) and for supplying a filtered pseudo noise sequence (**w**); and

means for adding said filtered pseudo noise sequence (**w**) to said data (**x**).

7. Device according to Claim 6, further comprising:

first means of pseudo random interleaving of the data (**x**) representative of the content to be protected so as to supply interleaved data ($\tilde{\mathbf{x}}$), said interleaved data being supplied to the addition means so as to be added to the filtered pseudo noise sequence (**w**); and

means of inverse interleaving of said first interleaving means, linked to the output of said addition means so as to supply the watermarked data.

8. Device according to Claim 6, comprising:

means for transforming the content to be protected into data (**x**) representative of said content;

means for generating a modulation sequence (**m**) indicative of the maximum amount of noise which can be added to said data;

wherein:

first means of pseudo random interleaving of said data (**x**) representative of the content to be protected so as to supply interleaved data ($\tilde{\mathbf{x}}$);

second means of pseudo random interleaving, which are identical to the first adapted for receiving said modulation sequence (**m**) so as to supply an interleaved modulation sequence ($\tilde{\mathbf{m}}$);

multiplication means adapted for receiving, on the one hand the interleaved modulation sequence ($\tilde{\mathbf{m}}$), and on the other hand the filtered pseudo noise sequence (**w**), so as to supply the watermark;

means of addition of the interleaved data ($\tilde{\mathbf{x}}$) and of the watermark, the output of said addition means being linked to:

means of inverse interleaving of said first and second interleaving means so as to supply the watermarked data (**y**); and

means of inverse transformation of the watermarked data into a marked content.

9. Device for detecting a watermark in data (**r**) representing a content received, comprising:

means for estimating the power spectral density of said data; and

means of likelihood testing of hypotheses so as to estimate whether said data include a pseudo noise sequence which has been filtered by a filter with predefined spectral response (H(f)).

10. Device according to Claim 9, adapted for detecting a watermark inserted by an insertion device wherein:

means of pseudo random interleaving of the data (**r**) representing the content received, which are adapted for performing the same interleaving (p) as said first interleaving means of the insertion device, said interleaved data ($\tilde{\mathbf{r}}$) being supplied to said means for estimating the power spectral density.

11. Device according to Claim 10, adapted for detecting a watermark inserted by an insertion device wherein:

means for transforming the content received into data (**r**) representative of said content, said transforming means being adapted for performing the same transformation as the transforming means of the insertion device.

IN THE ABSTRACT:

Please add the following Abstract.

-- The watermarking system uses a first series of parameters, the private key, for the insertion of the watermark, and a second series of parameters, the public key, for the detection of the watermark, so that knowledge of the public key does not make it possible to know the private key and does not make it possible to delete or modify the watermark. The insertion of the watermark is performed by adding a pseudo random noise sequence, filtered by a filter with impulse response, to the data to be watermarked. The detection of the watermark is performed by searching through the data received for whether they contain noise which has been filtered by a filter with predefined spectral response. Application to copy protection.--

REMARKS

The specification has been amended to include a reference to the priority applications.

The claims have been amended to remove reference indicia and to meet the requirement of the United States.

To meet the requirements of the United States, the Abstract (as originally filed in the PCT application) is added.

No fee is believed to have been incurred by virtue of this amendment. However if a fee is incurred on the basis of this amendment, please charge such fee against deposit account 07-0832

Respectfully submitted,
Teddy Furon
Pierre Duhamel

David T. Shoneman
Attorney for Applicant
Registration No. 39,371
609/734-9875

THOMSON multimedia Licensing Inc.
Patent Operation
PO Box 5312
Princeton, NJ 08543-5312

November 20, 2001

MARKED UP VERSION OF THE AMENDED CLAIMS

1.(AMENDED) Method for inserting a watermark into data (**x**) representing a content to be protected, [characterized in that it comprises the steps consisting in] comprising the steps of:

a) supplying a pseudo random noise sequence (**v**) to the input of a filter with predefined impulse response (**h**); and

b) adding said filtered pseudo noise sequence (**w**) to said data.

2.(AMENDED) Method according to Claim 1, [characterized in that it furthermore comprises the steps consisting in] further comprising the steps of:

c) performing a pseudo random interleaving (p) of the data (**x**) before step b); and

d) performing an inverse interleaving after step b) so as to obtain the watermarked data.

3.(AMENDED) Method for detecting a watermark in data (**r**) representing a content received, [characterized in that it comprises the steps consisting in] comprising the steps of:

i) performing a spectral analysis of said data; and

ii) deducing therefrom whether said data include a pseudo noise sequence which has been filtered by a filter with predefined spectral response (H(f)).

4.(AMENDED) Method according to Claim 3 for detecting a watermark in data (**r**) representing a content received, the watermark being adapted to be inserted in accordance with the method according to Claim 2, [characterized in that it furthermore comprises a step consisting in] further comprising:

iii) performing, before step i), a pseudo random interleaving (p) of the data (**r**) received, which is identical to the interleaving performed in step c).

5.(AMENDED) Watermarking System using a watermark insertion method according to [one of Claims 1 or 2] Claim 1 and a watermark detection method according to [one of Claims 3 or 4, characterized in that] Claim 3, wherein a first series of parameters (**v**, **h**), the private key (K_{PRI}), is used for the insertion of the watermark and a second series of parameters (|H(f)|), the public key (K_{PUB}), is used for the detection of the watermark, so that:

knowledge of the public key does not make it possible to know the private key; and

knowledge of the watermark detection method and of the public key does not make it possible to delete or modify the watermark.

6.(AMENDED) Device for inserting a watermark into data (**x**) representing a content to be protected, [characterized in that it comprises] comprising:

means for generating a pseudo random noise sequence (**v**);

filtering means [(16)] having a predefined impulse response (**h**) and which are adapted for receiving said pseudo noise sequence (**v**) and for supplying a filtered pseudo noise sequence (**w**); and

- means [(22)] for adding said filtered pseudo noise sequence (**w**) to said data (**x**).

7.(AMENDED) Device according to Claim 6, [characterized in that it furthermore comprises] comprising:

first means [(20)] of pseudo random interleaving of the data (**x**) representative of the content to be protected so as to supply interleaved data ($\tilde{\mathbf{x}}$), said interleaved data being supplied to the addition means [(22)] so as to be added to the filtered pseudo noise sequence (**w**); and

means [(24)] of inverse interleaving of said first [(20)] interleaving means, linked to the output of said addition means [(22)] so as to supply the watermarked data.

8.(AMENDED) Device according to Claim 6, comprising:

means [(10)] for transforming the content to be protected into data (**x**) representative of said content;

means [(12)] for generating a modulation sequence (**m**) indicative of the maximum amount of noise which can be added to said data;

[characterized in that it furthermore comprises] wherein:

first means [(20)] of pseudo random interleaving of said data (**x**) representative of the content to be protected so as to supply interleaved data ($\tilde{\mathbf{x}}$);

second means [(14)] of pseudo random interleaving, which are identical to the first [(20)] adapted for receiving said modulation sequence (**m**) so as to supply an interleaved modulation sequence ($\tilde{\mathbf{m}}$);

multiplication means [(18)] adapted for receiving, on the one hand the interleaved modulation sequence ($\tilde{\mathbf{m}}$), and on the other hand the filtered pseudo noise sequence (**w**), so as to supply the watermark;

means [(22)] of addition of the interleaved data ($\tilde{\mathbf{x}}$) and of the watermark, the output of said addition means being linked to:

means [(24)] of inverse interleaving of said first [(20)] and second [(14)] interleaving means so as to supply the watermarked data (**y**); and

means [(26)] of inverse transformation of the watermarked data into a marked content.

9.(AMENDED) Device for detecting a watermark in data (**r**) representing a content received, [characterized in that it comprises] comprising:

means [(34)] for estimating the power spectral density of said data; and

means [(36)] of likelihood testing of hypotheses so as to estimate whether said data include a pseudo noise sequence which has been filtered by a filter with predefined spectral response (H(f)).

10.(AMENDED) Device according to Claim 9, adapted for detecting a watermark inserted by an insertion device [according to one of Claims 7 or 8, characterized in that it comprise] wherein:

means [(32)] of pseudo random interleaving of the data (**r**) representing the content received, which are adapted for performing the same interleaving (p) as said first interleaving means [(20)] of the insertion device, said interleaved data ($\tilde{\mathbf{r}}$) being supplied to said means [(34)] for estimating the power spectral density.

11.(AMENDED) Device according to Claim 10, adapted for detecting a watermark inserted by an insertion device [according to Claim 8, characterized in that it furthermore comprises] wherein:

means [(30)] for transforming the content received into data (**r**) representative of said content, said transforming means being adapted for performing the same transformation as the transforming means [(10)] of the insertion device.

Digital data watermarking system using novel watermark insertion and detection methods

The present invention relates to the field of watermarking of digital data. It relates more particularly to a system for watermarking data using novel watermark insertion and detection methods as well as to devices for implementing these methods.

Recent methods for protecting against the illicit copying of digital data use the principle of data watermarking which consists in inserting a marking item, commonly referred to as a "watermark", into a multimedia content (still image, video, sound, etc.) in an imperceptible manner. The watermark can for example be a signal indicating that the content may not be copied or any other item allowing the supplier of the multimedia content to detect illegal copies.

In order to play its role perfectly, the watermark must be robust to transformations of the watermarked content, whether these transformations be made intentionally by a pirate who wishes to erase the watermark, or whether they result from distortions which occurred during the transmission of the signal containing the watermarked data.

Various data watermarking techniques are known from the prior art. Reference may in particular be made to the documents EP-A-0 828 372, EP-A-0 840 513, WO-A-98/03014 or WO-A-98/54897 which describe methods for inserting watermarks into data to be protected and methods for detecting the presence of such watermarks in the data.

A scheme which is generally used to describe the principle of data watermarking is that of Figure 1. A first part 1 relates to the insertion of a hidden item W (the watermark) into a content to be protected C. This results in a watermarked content CT. Part 2 relates to the detection of the presence of the item W in the content received CT. An additional datum K is also necessary in the process for inserting and detecting the watermark. This datum K which must be shared in a secret manner by the device for inserting and detecting the watermark is referred to as the key by analogy with so-called symmetric or private-key cryptography systems.

For example, a known watermarking technique consists in adding a pseudo random noise sequence to data which are to be watermarked. The detection process is carried out, in this case, by performing a correlation calculation: the data received are declared watermarked if the correlation with the reference pseudo noise sequence (used for the insertion of the watermark) is greater than a given threshold. In this example, the reference pseudo noise sequence constitutes the key K of the data watermarking scheme of Figure 1.

The problem with this scheme is that each entity capable of detecting the watermark must share the same key K as the entity which inserted the watermark. In this case, the entity capable of detecting the watermark can furthermore delete it or modify it, thereby doing away with all the benefit of the initial watermarking of the data. Consequently, a supplier of content protected by watermarking should not communicate his key K, which served for the insertion of the watermark, other than in a secret manner to trusted entities. This considerably limits the possibilities of using data watermarking in numerous fields.

In particular, in the field of consumer electronic appliances, it is well known that it is almost impossible, at any event at reasonable cost, to store secret parameters in an appliance or in software contained in such an appliance. Smart cards, which are regarded as the only pieces of equipment allowing the secure storage of a secret parameter, are not themselves powerful enough to perform the calculations connected with a watermark detection process.

In the example described above where the watermarking is carried out by adding a pseudo random noise sequence to the data which are to be watermarked, even if the reference pseudo noise sequence is stored secretly in the watermark detection device, it has been demonstrated that a pirate can theoretically discover the reference sequence and thus delete the watermark from the data by observing the output from the detector as a function of a large number of different input signals.

The invention aims to solve the aforesaid problems.

To this end, the invention relates to a method for inserting a watermark into data representing a content to be protected. According to the invention, the method comprises the steps consisting in:

a) supplying a pseudo random noise sequence to the input of a filter with predefined impulse response; and

b) adding the filtered pseudo noise sequence to the data.

According to a preferred aspect of the invention, the method furthermore comprises the steps consisting in:

c) performing a pseudo random interleaving of the data before step b); and

d) performing an inverse interleaving after step b) so as to obtain the watermarked data.

The invention also relates to a method for detecting a watermark in data representing a content received, characterized in that it comprises the steps consisting in:

i) performing a spectral analysis of the data; and

ii) deducing therefrom whether the data include a pseudo noise sequence which has been filtered by a filter with predefined spectral response.

According to another preferred aspect of the invention, a pseudo random interleaving of the data received, which is identical to the interleaving performed in step c) above, is performed before step i).

The invention also relates to a system for watermarking data using a watermark insertion method and a watermark detection method as those above. According to the invention, a first series of parameters, the private key, is used for the insertion of the watermark and a second series of parameters, the public key, is used for the detection of the watermark, so that:

- knowledge of the public key does not make it possible to know the private key; and
- knowledge of the method of detection and of the public key does not make it possible to delete or modify the watermark.

The invention also relates to a device for inserting a watermark into data representing a content to be protected. According to the invention, the device comprises:

- means for generating a pseudo random noise sequence;
- filtering means having a predefined impulse response and which are adapted for receiving the pseudo noise sequence and for supplying a filtered pseudo noise sequence; and
- means for adding the filtered pseudo noise sequence to the data.

According to a preferred embodiment of the invention, the device furthermore comprises:

- first means of pseudo random interleaving of the data representative of the content to be protected so as to supply interleaved data, the interleaved data being supplied to the addition means so as to be added to the filtered pseudo noise sequence; and
- means of inverse interleaving of the first interleaving means, linked to the output of the said addition means so as to supply the watermarked data.

According to a particular embodiment of the invention, the device comprises:

- means for transforming the content to be protected into data representative of the content;

- means for generating a modulation sequence indicative of the maximum amount of noise which can be added to the data;

- first means of pseudo random interleaving of the data representative of the content to be protected so as to supply interleaved data;

- second means of pseudo random interleaving, which are identical to the first adapted for receiving the modulation sequence so as to supply an interleaved modulation sequence;

- multiplication means adapted for receiving, on the one hand the interleaved modulation sequence, and on the other hand the filtered pseudo noise sequence, so as to supply the watermark;

- means of addition of the interleaved data and of the watermark, the output of the addition means being linked to:

- means of inverse interleaving of the first and second interleaving means so as to supply the watermarked data; and

- means of inverse transformation of the watermarked data into a marked content.

The invention also relates to a device for detecting a watermark in data representing a content received. According to the invention, the device comprises:

- means for estimating the power spectral density of the data; and

- means of likelihood testing of hypotheses so as to estimate whether the data include a pseudo noise sequence which has been filtered by a filter with predefined spectral response.

According to a particular embodiment, the device furthermore comprises:

- means of pseudo random interleaving of the data representing the content received, which are adapted for performing the same interleaving as the first interleaving means of the insertion device, the interleaved data being supplied to the means for estimating the power spectral density.

According to another particular embodiment, the device furthermore comprises:

- means for transforming the content received into data representative of the content, the transforming means being adapted for performing the same transformation as the transforming means of the insertion device.

Other characteristics and advantages of the invention will become apparent on reading the following description of a particular embodiment, which is non-limiting, of the invention given with reference to the appended figures, among which:

- Figure 1, described previously, illustrates a known scheme for watermarking digital data;
- Figure 2 schematically represents a watermark insertion device according to the invention;
- Figure 3 schematically represents a watermark detection device according to the invention;
- Figure 4 illustrates a novel scheme for watermarking digital data according to the invention.

Represented schematically in Figure 2 is a device according to the invention for inserting a watermark into a signal representative of a content to be protected. This signal can in particular be a digital video or audio signal or else a signal representing a still image such as a photograph or a computer-calculated synthetic image, or more generally, any signal representing a multimedia content.

Firstly, the content to be protected is transformed by a transformation module 10 into a sequence of digital data $\mathbf{x} = \{x_n\}$, n lying between 1 and N. For example, if the content to be protected is an image comprising N pixels, the coefficients x_n can correspond to the luminance of each pixel of the image. These may also be coefficients of a Discrete Fourier Transform of the signal representing the content to be protected, or else coefficients of a Fourier-Mellin Transform or coefficients of a wavelet decomposition when the content to be protected is a still image.

The data sequence $\mathbf{x}$ representing the content to be protected is transmitted on the one hand to a module HPM 12 which outputs a modulation sequence $\mathbf{m} = \{m_n\}$, $\forall n \in [1..N]$. The module HPM calculates this modulation sequence as a function of algorithms based on human perception models, such as Sarnoff's model of the eye. This sequence $\mathbf{m} = \{m_n\}$ represents the maximum amount of noise which can be added to each coefficient x_n without perceptible loss of quality.

According to one aspect of the invention, the data sequence $\mathbf{x}$ is transmitted moreover to an interleaver 20, which performs a random permutation p of the coefficients x_n so as to supply a sequence of interleaved coefficients $\tilde{\mathbf{x}} = \{x_{p(n)}\}$. The purpose of this interleaving of the data sequence $\mathbf{x}$ will be explained subsequently.

The modulation sequence $\mathbf{m}$ is also transmitted to an interleaver 14 which performs the same permutation p of the coefficients m_n as that performed by the interleaver 20 so as to output an interleaved modulation sequence $\tilde{\mathbf{m}} = \{m_{p(n)}\}$.

In order to constitute the watermark which will be inserted into the data sequence $\mathbf{x}$ representing the content to be protected, a pseudo random noise generator (not represented) firstly supplies a pseudo noise sequence $\mathbf{v} = \{v_n\}$, $\forall n \in [1..N]$, with Gaussian distribution. This pseudo noise sequence $\mathbf{v}$ is transmitted to the input of a filter 16, of Linear Time Invariant (LTI) type, whose impulse response is:

$\mathbf{h} = \{h_n\}$, $\forall n \in [1..L]$ where L is an integer corresponding to the length of the filter;

and whose spectral response is H(f), H(f) being the Fourier Transform of $\mathbf{h}$.

At the output of the filter 16 one obtains a filtered pseudo noise sequence $\mathbf{w} = \{w_n\}$, $\forall n \in [1..N]$ satisfying the following equation (1):

$$w_n = \sum_{k=1}^{L} v_{n-k} \cdot h_k = h_n \otimes v_n \qquad \forall n \in [1..N] \qquad (1)$$

in which $\otimes$ represents the convolution product.

From this may be deduced, from the interference theorem, the following two equations (2) and (3):

$$\varphi_{ww}(\tau) = (\mathbf{h} \otimes \mathbf{h}) \otimes \varphi_{vv}(\tau) \qquad (2)$$

in which $\varphi_{ww}(\tau)$ and $\varphi_{vv}(\tau)$ respectively represent the auto-correlation functions of **w** and of **v**; and

$$\Phi_{ww}(f) = |H(f)|^2 \cdot \Phi_{vv}(f) \qquad (3)$$

in which $\Phi_{ww}(f)$ and $\Phi_{vv}(f)$ respectively represent the power spectral densities of $\varphi_{ww}(\tau)$ and $\varphi_{vv}(\tau)$, that is to say their Fourier Transforms.

Since **v** is a pseudo random noise sequence with Gaussian distribution, its spectrum, that is to say the function $\Phi_{vv}(f)$, has a substantially flat shape. On the other hand, once this sequence **v** is filtered by the filter 16, the resulting sequence **w** exhibits a spectrum $\Phi_{ww}(f)$ which is no longer flat on account of the term $|H(f)|^2$. It is also important to note, so as to comprehend the rest of the invention, that knowledge of $|H(f)|^2$ (and by the same token, knowledge of the modulus of H(f):|H(f)|) does not make it possible to retrieve H(f) (and hence **h**) since there is an uncertainty with regard to the phase of H(f).

Returning to Figure 2, the filtered pseudo noise sequence **w** is multiplied (multiplier 18) by the interleaved modulation sequence $\tilde{\mathbf{m}}$ and the resulting sequence, which constitutes the watermark, is added (adder 22) to the sequence of interleaved data $\tilde{\mathbf{x}}$.

The output sequence from the adder 22 is denoted $\tilde{\mathbf{y}} = \{y_{p(n)}\}$ and satisfies the following equations (4) and (5):

$$y_{p(n)} = x_{p(n)} + m_{p(n)} \cdot (h_n \otimes v_n) \qquad (4)$$

$$\tilde{\mathbf{y}} = \tilde{\mathbf{x}} + \tilde{\mathbf{m}} \cdot (\mathbf{h} \otimes \mathbf{v}) \qquad (5)$$

The power spectral density of the sequence of watermarked interleaved data $\tilde{\mathbf{y}}$ is given by the following equations (6) and (7):

$$\Phi_{\tilde{\mathbf{y}}\tilde{\mathbf{y}}}(f) = \Phi_{\tilde{\mathbf{x}}\tilde{\mathbf{x}}}(f) + \Phi_{\tilde{\mathbf{m}}\tilde{\mathbf{m}}}(f) \cdot \Phi_{\mathbf{h}\otimes\mathbf{v}}(f) \qquad (6)$$

$$\Phi_{\tilde{\mathbf{y}}\tilde{\mathbf{y}}}(f) = \left(\mu_x^2 \cdot \delta(f) + \sigma_x^2\right) + \left(\sigma_m^2 \cdot \sigma_v^2 \cdot \sum_u h_u^2\right) + \mu_m^2 \cdot \sigma_v^2 \cdot |H(f)|^2 \qquad (7)$$

In equation (7), μ_j and σ_j respectively represent the mean and the standard deviation of the sequence $\mathbf{j} = \{j_n\}$ with $j \in \{x, m, v\}$, $\delta(f)$ corresponds to the Dirac pulse and the expression $\left(\sigma_m^2 \cdot \sigma_v^2 \cdot \sum_u h_u^2\right)$ is equal to a constant.

The sequence of watermarked interleaved data $\tilde{\mathbf{y}}$ is then transmitted to an inverse interleaver 24 which performs the operation inverse to the permutation p performed by the interleavers 20 and 14 so as to supply a sequence of watermarked data $\mathbf{y} = \{y_n\}$ whose coefficients are in the same order as the initial order of the data $\mathbf{x} = \{x_n\}$.

A transformation inverse to that performed by the transformation module 10 is then performed by the module 26 so as to obtain the marked content (or watermarked content) which is thus protected against illicit copying without the watermark being perceptible within the content.

We shall now describe, in conjunction with Figure 3, a device for detecting a watermark in a received content when this watermark has been inserted into a content to be protected by a device such as that of Figure 2.

The principle of the detection is based on the spectral analysis of the signal received.

The signal received is representative of the received content for which one will seek to determine whether or not it is watermarked. This content is of the same type as the content to be protected described previously. In the example which follows, it will be assumed that the content received is an image containing N pixels.

The content received is firstly transmitted to a transformation module 30 which performs the same transformation operation as the module 10 of the watermark insertion device of Figure 2 so as to supply a data sequence $\mathbf{r} = \{r_n\}$, $\forall n \in [1..N]$ representing the content received. In our example, it is assumed that the luminances r_n of the pixels of the image received are obtained as output from the transformation module 30.

If the content received were to correspond exactly to the watermarked content emanating from the device of Figure 2, that is to say if no transformation or distortion of the signal had taken place during transmission between the watermark insertion device and the detection device, then one would have:

$$\mathbf{r} = \{r_n\} = \mathbf{y} = \{y_n\}$$

In practice, this is not always the case since the signal sometimes undergoes transformations during its transmission.

Since the watermark has been inserted, in the device of Figure 2, into a sequence of interleaved data $\tilde{\mathbf{x}}$, the data sequence $\mathbf{r}$ will, in order to detect the possible presence of a watermark in the content received, be transmitted to an interleaver 32 performing the same permutation p of the coefficients r_n as that performed by the interleavers 20 and 14 of Figure 2.

A sequence of interleaved data $\tilde{\mathbf{r}} = \{r_{p(n)}\}$ is obtained as output from the interleaver 32.

It was seen previously that when the watermark inserted is a pseudo noise sequence filtered by a filter with impulse response $\mathbf{h}$ and with spectral response H(f), the power spectral density of the (interleaved) data obtained $\tilde{\mathbf{y}}$ is expressed by relations (6) and (7).

The purpose of the interleaving of the data sequence $\mathbf{x}$ and of the modulation sequence $\mathbf{m}$ will now be apparent. Indeed, if the data sequence $\mathbf{x}$ represents the pixels of an image, its spectral density has a very structured shape with very large amplitude differences. The role of the interleaving of the data is to sever the statistical coherence of this sequence so that the spectral density of the sequence of interleaved data $\tilde{\mathbf{x}}$ has a substantially flat shape, such as that of a pseudo noise sequence with Gaussian distribution.

Thus, if a watermark consisting of a pseudo noise sequence filtered by a filter with spectral response H(f) is added to this interleaved sequence, a data sequence is obtained whose power spectral density can be expressed by relation (7) in which the significant term $|H(f)|^2$ can be detected.

The principle of the detection will therefore be based on the spectral analysis of the sequence $\tilde{\mathbf{r}}$ and on a Maximum Likelihood Ratio Hypothesis test (MLR Hypothesis test), the hypothesis tested being the following: if the sequence of interleaved data $\tilde{\mathbf{r}}$ contains noise, is it noise which has been filtered by a filter whose spectral response has a modulus similar to $|H(f)|$? If the response is yes, one will deduce from this that the noise present in the sequence $\tilde{\mathbf{r}}$ is a watermark and, in the contrary case, one will conclude from this that the content received was not watermarked.

In practice, this analysis is based on calculations relating to spectral analysis and the likelihood testing of hypotheses which are described in detail in the work by K. Dzhaparidze, *"Parameter Estimation and Hypothesis Testing in Spectral Analysis of Stationary Time Series"*, Springer Series in Statistics, Springer-Verlag, 1986, to which reference may be made for further details.

Returning to Figure 3, the sequence of received interleaved data $\tilde{r}$ is transmitted to a module 34 performing a Periodogram calculus. This calculus is aimed at estimating the power spectral density of the sequence $\tilde{r}$. A quantity $I_N(f)$ given by the following relation (8)

$$I_N(f)=\frac{1}{N}\left|\sum_{k=1}^{N}\tilde{r}_k\cdot\exp(2\pi jfk)\right|^2 \tag{8}$$

is obtained at output.

This quantity is then transmitted to a module 36 performing a MLR Hypothesis test so as to determine whether the content received is watermarked (output response "Y") or not (output response "N").

The module 36 tests the likelihood of two hypotheses:

- according to the first hypothesis G_0, the content received is not watermarked, hence the spectral density of the sequence $\tilde{r}$ is substantially flat and can be estimated via the following relation (9):

$$g_0(f)=\sigma_r^2+\mu_r^2\cdot\delta(f) \tag{9}$$

- according to the second hypothesis G_1, the content received is watermarked and the spectral density of the sequence $\tilde{r}$ can be estimated via the following relation (10):

$$g_1(f)=\mu_m^2\cdot\sigma_v^2\cdot|H(f)|^2+C \tag{10}$$

in which C is a constant and σ_v is equal to 1 (one preferably chooses the pseudo noise sequence **v** at the level of the insertion device so that σ_v is equal to 1, but one may equally choose other values). Furthermore, μ_m is normed at the level of the insertion device and equals for example 3.

To estimate the likelihood of the hypotheses G_0 and G_1, the module 36 calculates two numbers $U_{N,0}(\tilde{r})$ and

$U_{N,1}(\tilde{r})$ representing the likelihoods of the hypotheses G_0 and G_1 according to the following relation (11):

$$U_{N,i}(\tilde{r}) = -\int_{-\frac{1}{2}}^{\frac{1}{2}} \left(\log g_i(f) + \frac{I_N(f)}{g_i(f)} \right) df \quad \text{with } i \in \{0,\ 1\} \quad \textbf{(11)}$$

By then comparing these two numbers, the module 36 deduces from this:

- if $U_{N,1}(\tilde{r}) > U_{N,0}(\tilde{r})$, then the response of the detector is "Y" signifying that the content received is watermarked; and

- if $U_{N,1}(\tilde{r}) < U_{N,0}(\tilde{r})$, then the response of the detector is "N" signifying that the content received is not watermarked.

It is also possible, in a preferential manner, to calculate the difference $(U_{N,1}(\tilde{r}) - U_{N,0}(\tilde{r}))$ and to perform the above comparisons only if this difference is greater than a predetermined threshold, this being so as to guarantee better exactness of detection.

The watermark insertion and detection methods just described with reference to Figures 2 and 3 make it possible to produce a novel watermarking system which is illustrated by Figure 4. In this novel system and according to a preferred aspect of the invention, a parameter which is referred to as the "private key" K_{PRI} is used for the insertion (100) of a watermark W into a content C, whereas another parameter which is referred to as the "public key" K_{PUB} is used for the detection (200) of a watermark in a content received CT. The terms "private key" and "public key" are used by analogy with public key crytographic systems. It will be noted that here the watermark W is binary, that is to say that, either the content C is watermarked, or it is not, but W does not contain any item of its own.

In the embodiment described above, the private key K_{PRI} is formed by the pseudo random noise sequence $\mathbf{v}$ as well as by the impulse response $\mathbf{h}$ of the filter 16 (Fig. 2). The sequences $\mathbf{v} = \{v_n\}$ and $\mathbf{h} = \{h_n\}$ are in effect indispensable to the calculation of the sequence

$\mathbf{w} = \{w_n\}$ which is itself, after having been multiplied by the interleaved modulation sequence $\tilde{\mathbf{m}}$, inserted into the data representing the content to be protected.

The public key used to detect the watermark in the content received is for its part formed from the modulus of the spectral response of the filter 16 $|H(f)|$. Indeed, in the spectral analysis calculations performed (modules 34 and 36 of Figure 3) to detect the presence of a watermark in a content received CT, only the knowledge of $|H(f)|$ is necessary. In particular, it is not necessary to know **v** and **h** (the private key) to perform the detection of the watermark. In actual fact, as was seen earlier in the description, the knowledge of $|H(f)|$ does not suffice to know $H(f)$ and hence **h**.

A system is therefore obtained in which knowledge of the public key does not make it possible to deduce the private key from this. Also, not knowing the private key, it is impossible for the device performing the detection of the watermark to delete it or to modify it. The detection can therefore be performed in a non-secure environment with no risk of the watermark being erased.

CLAIMS

1. Method for inserting a watermark into data (**x**) representing a content to be protected, characterized in that it comprises the steps consisting in:

a) supplying a pseudo random noise sequence (**v**) to the input of a filter with predefined impulse response (**h**); and

b) adding said filtered pseudo noise sequence (**w**) to said data.

2. Method according to Claim 1, characterized in that it furthermore comprises the steps consisting in:

c) performing a pseudo random interleaving (p) of the data (**x**) before step b); and

d) performing an inverse interleaving after step b) so as to obtain the watermarked data.

3. Method for detecting a watermark in data (**r**) representing a content received, characterized in that it comprises the steps consisting in:

i) performing a spectral analysis of said data; and

ii) deducing therefrom whether said data include a pseudo noise sequence which has been filtered by a filter with predefined spectral response (H(f)).

4. Method according to Claim 3 for detecting a watermark in data (**r**) representing a content received, the watermark being adapted to be inserted in accordance with the method according to Claim 2, characterized in that it furthermore comprises a step consisting in:

iii) performing, before step i), a pseudo random interleaving (p) of the data (**r**) received, which is identical to the interleaving performed in step c).

5. Watermarking System using a watermark insertion method according to one of Claims 1 or 2 and a watermark detection method according to one of Claims 3 or 4, characterized in that a first series of

parameters (**v**, **h**), the private key (K_{PRI}), is used for the insertion of the watermark and a second series of parameters (|H(f)|), the public key (K_{PUB}), is used for the detection of the watermark, so that:

- knowledge of the public key does not make it possible to know the private key; and

- knowledge of the watermark detection method and of the public key does not make it possible to delete or modify the watermark.

6. Device for inserting a watermark into data (**x**) representing a content to be protected, characterized in that it comprises:

- means for generating a pseudo random noise sequence (**v**);

- filtering means (16) having a predefined impulse response (**h**) and which are adapted for receiving said pseudo noise sequence (**v**) and for supplying a filtered pseudo noise sequence (**w**); and

- means (22) for adding said filtered pseudo noise sequence (**w**) to said data (**x**).

7. Device according to Claim 6, characterized in that it furthermore comprises:

- first means (20) of pseudo random interleaving of the data (**x**) representative of the content to be protected so as to supply interleaved data ($\tilde{\mathbf{x}}$), said interleaved data being supplied to the addition means (22) so as to be added to the filtered pseudo noise sequence (**w**); and

- means (24) of inverse interleaving of said first (20) interleaving means, linked to the output of said addition means (22) so as to supply the watermarked data.

8. Device according to Claim 6, comprising:

- means (10) for transforming the content to be protected into data (**x**) representative of said content;

- means (12) for generating a modulation sequence (**m**) indicative of the maximum amount of noise which can be added to said data;

characterized in that it furthermore comprises:

- first means (20) of pseudo random interleaving of said data ($\mathbf{x}$) representative of the content to be protected so as to supply interleaved data ($\tilde{\mathbf{x}}$);

- second means (14) of pseudo random interleaving, which are identical to the first (20) adapted for receiving said modulation sequence ($\mathbf{m}$) so as to supply an interleaved modulation sequence ($\tilde{\mathbf{m}}$);

- multiplication means (18) adapted for receiving, on the one hand the interleaved modulation sequence ($\tilde{\mathbf{m}}$), and on the other hand the filtered pseudo noise sequence ($\mathbf{w}$), so as to supply the watermark;

- means (22) of addition of the interleaved data ($\tilde{\mathbf{x}}$) and of the watermark, the output of said addition means being linked to:

- means (24) of inverse interleaving of said first (20) and second (14) interleaving means so as to supply the watermarked data ($\mathbf{y}$); and

- means (26) of inverse transformation of the watermarked data into a marked content.

9. Device for detecting a watermark in data ($\mathbf{r}$) representing a content received, characterized in that it comprises:

- means (34) for estimating the power spectral density of said data; and

- means (36) of likelihood testing of hypotheses so as to estimate whether said data include a pseudo noise sequence which has been filtered by a filter with predefined spectral response (H(f)).

10. Device according to Claim 9, adapted for detecting a watermark inserted by an insertion device according to one of Claims 7 or 8, characterized in that it comprises:

- means (32) of pseudo random interleaving of the data ($\mathbf{r}$) representing the content received, which are adapted for performing the same interleaving (p) as said first interleaving means (20) of the insertion device, said interleaved data ($\tilde{\mathbf{r}}$) being supplied to said means (34) for estimating the power spectral density.

11. Device according to Claim 10, adapted for detecting a watermark inserted by an insertion device according to Claim 8, characterized in that it furthermore comprises:

- means (30) for transforming the content received into data (**r**) representative of said content, said transforming means being adapted for performing the same transformation as the transforming means (10) of the insertion device.

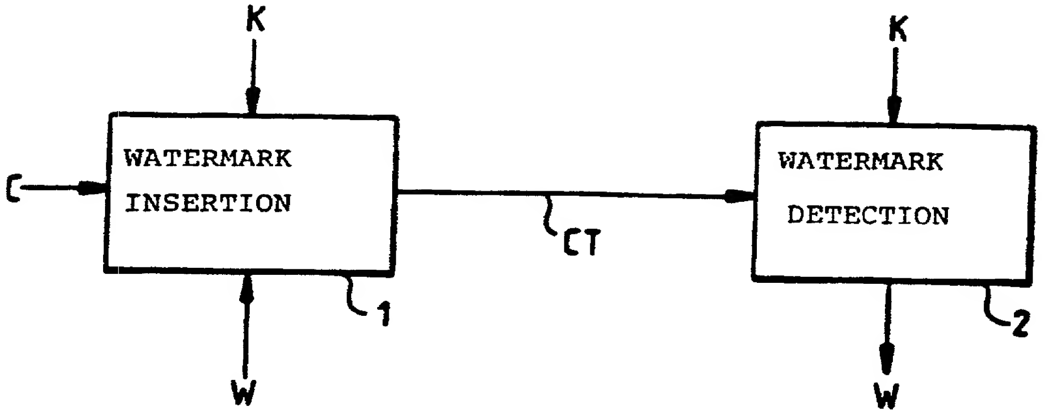
K
K
C
WATERMARK
INSERTION
CT
WATERMARK
DETECTION
1
2
W
W

FIG.1

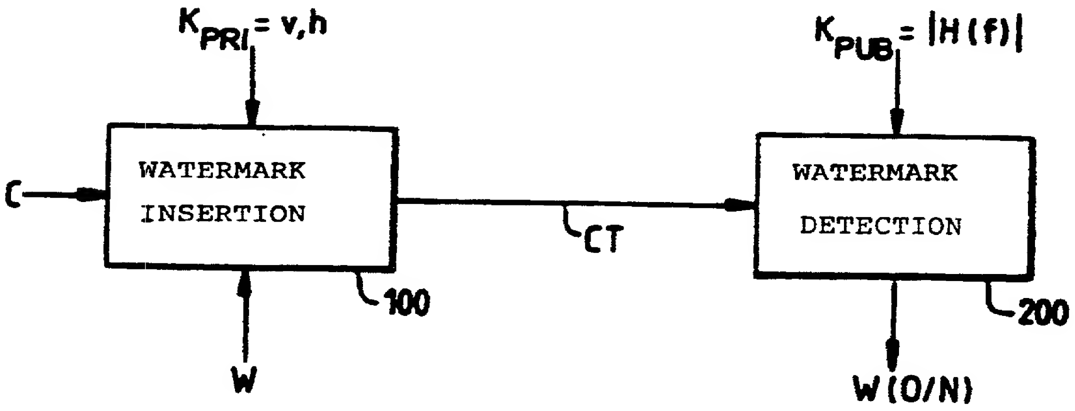
K_{PRI} = v,h
K_{PUB} = |H(f)|
C
WATERMARK
INSERTION
CT
WATERMARK
DETECTION
100
200
W
W(O/N)

FIG.4

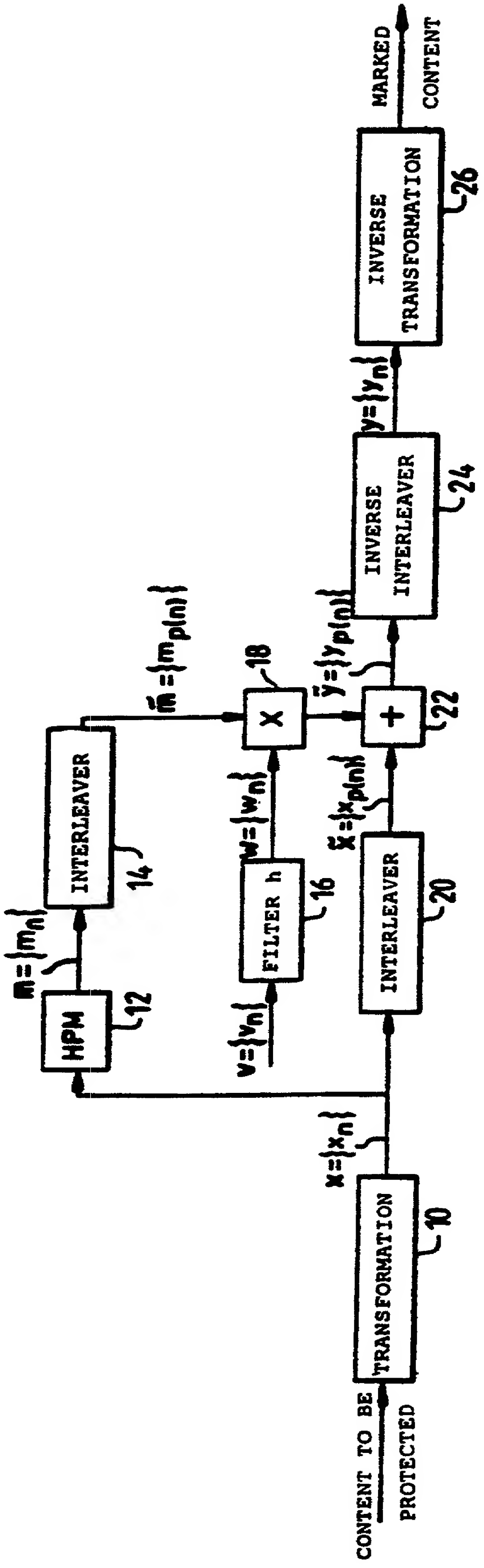
CONTENT TO BE PROTECTED
TRANSFORMATION
10
$x=\{x_n\}$
HPM
12
$m=\{m_n\}$
INTERLEAVER
14
$\tilde{m}=\{m_{p(n)}\}$
$v=\{v_n\}$
FILTER h
16
$w=\{w_n\}$
X
18
INTERLEAVER
20
$\tilde{x}=\{x_{p(n)}\}$
+
22
$\tilde{y}=\{y_{p(n)}\}$
INVERSE INTERLEAVER
24
$y=\{y_n\}$
INVERSE TRANSFORMATION
26
MARKED CONTENT

FIG. 2

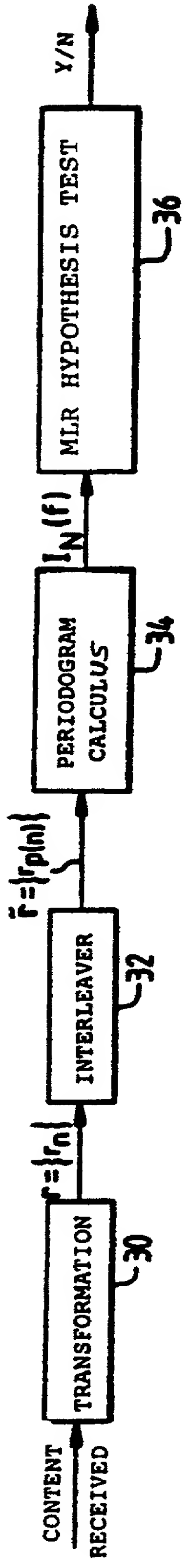
CONTENT RECEIVED
TRANSFORMATION
30
$r=\{r_n\}$
INTERLEAVER
32
$\tilde{r}=\{r_{p(n)}\}$
PERIODOGRAM CALCULUS
34
$I_N(f)$
MLR HYPOTHESIS TEST
36
Y/N

FIG. 3

DECLARATION FOR UNITED STATES PATENT APPLICATION,
POWER OF ATTORNEY, DESIGNATION OF CORRESPONDENCE ADDRESS

As a below named inventor, I hereby declare that my residence, post office address and citizenship are as stated below next to my name, and that I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

DIGITAL DATA WATERMARKING SYSTEM USING NOVEL WATERMARK INSERTION AND DETECTION METHODS

the specification of which
(CHECK ONE) ( ) is attached hereto.
(XX) was filed on May 5, 2000, Application Serial. No.PCT/EP00/04053
and was amended on .

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with 37 CFR 1.56(a).

I hereby claim foreign priority benefits under 35 USC 119 of any foreign application(s) for patent, utility model, design or inventor's certificate having a filing date before that of the application(s) on which priority is claimed:

Prior Foreign Application(s)			Priority Claimed	
Number	Country	Date Filed	Yes	No
9907139	FR	June 1, 1999	xx	

I hereby claim the benefit under 35 USC 120 of any US Application(s) listed below, and, insofar as the subject matter of each of the claims of this Application is not disclosed in the prior US application in the manner provided by the first paragraph of 35 USC 112, I acknowledge the duty to disclose information which is material to the examination of this application in accordance with 37 CFR 1.56(a).

Serial No.: Filed:

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that wilful false statements and the like so made are punishable by fine or imprisonment, or both, under of 18 USC 1001 and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

I hereby appoint the following attorneys to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith: Joseph S. Tripoli (Reg. No. 26,040), Dennis H. Irlbeck (Reg. No. 26,372), Eric Herrmann (Reg. No. 29,169) and Joseph J. Laks (Reg. No. 27,914) Telephone: (609) 734-9813.

4

Address all correspondence to Joseph S. Tripoli, Patent Operations - Thomson multimedia Licensing, Inc. - CN 5312 - Princeton, New Jersey 08543-0028.

Signature: Date: 11th day of October ,2001.
Sole or First Joint Inventor: Teddy Furon
Citizenship: FR
Residence and Post Office Address: 13 rue de la Santé
F- 35000 Rennes
France

Signature: Date: ______day of______________,2001.
Sole or First Joint Inventor: Pierre Duhamel
Citizenship: FR
Residence and Post Office Address: 25 rue du Coteau
F-92350 Le Plessis Robinson
France

(2)
Over

DECLARATION FOR UNITED STATES PATENT APPLICATION,
POWER OF ATTORNEY, DESIGNATION OF CORRESPONDENCE ADDRESS

As a below named inventor, I hereby declare that my residence, post office address and citizenship are as stated below next to my name, and that I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

DIGITAL DATA WATERMARKING SYSTEM USING NOVEL WATERMARK INSERTION AND DETECTION METHODS

the specification of which
(CHECK ONE) ( ) is attached hereto.
(XX) was filed on May 5, 2000, Application Serial. No.PCT/EP00/04053
and was amended on .

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with 37 CFR 1.56(a).

I hereby claim foreign priority benefits under 35 USC 119 of any foreign application(s) for patent, utility model, design or inventor's certificate having a filing date before that of the application(s) on which priority is claimed:

Prior Foreign Application(s)			Priority Claimed	
Number	Country	Date Filed	Yes	No
9907139	FR	June 1, 1999	xx	

I hereby claim the benefit under 35 USC 120 of any US Application(s) listed below, and, insofar as the subject matter of each of the claims of this Application is not disclosed in the prior US application in the manner provided by the first paragraph of 35 USC 112, I acknowledge the duty to disclose information which is material to the examination of this application in accordance with 37 CFR 1.56(a).

Serial No.: Filed:

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that wilful false statements and the like so made are punishable by fine or imprisonment, or both, under of 18 USC 1001 and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

I hereby appoint the following attorneys to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith: Joseph S. Tripoli (Reg. No. 26,040), Dennis H. Irlbeck (Reg. No. 26,372), Eric Herrmann (Reg. No. 29,169) and Joseph J. Laks (Reg. No. 27,914) Telephone: (609) 734-9813.

Address all correspondence to Joseph S. Tripoli, Patent Operations - Thomson multimedia Licensing, Inc. - CN 5312 - Princeton, New Jersey 08543-0028.

Signature: ______________________ Date: _____day of______________,2001.
Sole or First Joint Inventor: Teddy Furon
Citizenship: FR
Residence and Post Office Address:
13 rue de la Santé
F- 35000 Rennes
France

Signature: ______________________ Date: 12th day of October ,2001.
2-00 Sole or First Joint Inventor: Pierre Duhamel
Citizenship: FR
Residence and Post Office Address:
25 rue du Coteau
F-92350 Le Plessis Robinson FRX
France